Quantum Information and Computation

draft of notes 2013

Nicolas Macris

Contents

Preface

Draft of course notes

Part I

Quantum Mechanics and Quantum Bits

1 Experiments with light

At the beginning of the 20th century a major change of paradigm occured in the laws of physics. This revolution was triggered by a host of experimental discoveries which lead to a major revision of our concepts of particle, wave and measurements of observables such as for example position, velocity, magnetic moment. The quantum theory that emerged is today the best tested theory of physical phenomena. The classical laws of physics are seen as a limiting case of quantum laws, that are valid when quantum effects can be neglected. This is the case for a wide range of phenomena which roughly speaking are macroscopic phenomena for which Newton's (or perhaps relativistic) laws of motion and Maxwell equations are adequate. Quantum effects cannot be neglected when we want to describe microscopic phenomena. But note that macroscopic quantum phenomena also exist and the borderline between classical and quantum behaviors is a deep, subtle and not totally solved problem. In any case, quantum theory explains the chemical bond, is thus at the basis of chemistry, it explains the stucture of the atom and the periodic table of elements, and is the basis for nuclear, particle and high energy physics. Quantum mechanics is also necessary to explain many properties of condensed matter for example metals, semi-conductors, magnets, superconductors, superfluids. Quantum mechanics is necessary to explain the interaction of matter and light.

Quantum mechanics was largely discovered by studying the interaction of matter with light. The early experiments of the 20th century, and some of the late 19th century, forced physicist to revise completely their views on the intimate nature of light and matter. It was gradually realized that light has both particle-like and wave-like behaviors. Similarly particles (e.g. the electron) have both particle-like and wave-like behaviors. Today we view these constituents of matter as entities called "quantum fields". Wave and particle behaviors are manifestations of the quantum fields.

The laws of physics are expressed in mathematical language. It is thus not so surprising that these conceptual revolutions were couched in a mathematical formalism that departs quite radically from the one of classical physics. For example Heisenberg was bold enough to represent observable and measurable quantities, such as position and velocity of an electron orbiting an atom, by "matrices" or "linear operators". From our modern perpective it is hard to appreciate why this was so bold. Let us just point out here that matrices were not part of the curriculum of physics students in the 1920's and that Heisenberg constructed the rule of matrix multiplication and other linear algebra facts by means of guessing at the laws of physics. He was guided by experiment, was a genius, and guessed right! The mathematical formalism of quantum mechanics has posed new interesting problems in functional analysis, geometry, group theory (today quantum information theory also offers new mathematical challenges).

The development of quantum mechanics in its modern form spans a period of at least 25-30 years between 1900 and 1930's. It is the achievement of many experimental and theoretical physicists. This was a golden age of discovery in physics full of surprising developments. It will not be possible to go through and understand the historical development of quantum mechanics in this course. Starting with chapter 2, the modern formalism of quantum mechanics is presented. This mathematical formalisation of the physical laws discovered by the founding fathers, was first clearly spelled out by Dirac and von Neumann around 1930-1932 in two influencial books, and has remained for the main part unchanged since then.

Before proceeding directly to the mathematical formalism it is nevertheless good to motivate it thanks to simple experiments that can be performed with light. The experiments are presented here as "thought experiments", but they can be performed in a real lab. We will gradually introduce some of the basic ideas of quantum mechanics through the discussion of these experiments. This is the goal of this chapter.

1.1 Electromagnetic waves

According to Maxwell (1862) and Hertz (1886), light is an electromagnetic wave of electric $\mathbf{E}(\mathbf{x}, t)$ and magnetic $\mathbf{B}(\mathbf{x}, t)$ fields freely oscillating in vacuum. The solutions of Maxwell equations in empty space are superpositions of monochromatic modes of frequency ω. A mode, or plane wave, propagating along the z axis, is given by

$$\mathbf{E}(\mathbf{x}, t) = Re\, \mathbf{E}_0\, e^{i(kz-\omega t)}, \qquad \mathbf{B}(\mathbf{x}, t) = \frac{1}{c}\hat{\mathbf{z}} \times \mathbf{E}(\mathbf{x}, t), \qquad \omega = ck \tag{1.1}$$

The amplitude vector $\mathbf{E}_0$ (thus $\mathbf{E}$ and $\mathbf{B}$ also) always belongs to the $(x, y) \perp z$ plane,

$$\mathbf{E}_0 = E_0 \begin{bmatrix} \cos\theta e^{i\delta_x} \\ \sin\theta e^{i\delta_y} \\ 0 \end{bmatrix} \tag{1.2}$$

The energy per unit time per unit surface that would be imparted to a material object by the wave, is given by the norm of the Poynting vector

$$\mathbf{S} = \epsilon_0 c^2 \mathbf{E} \times \mathbf{B} \tag{1.3}$$

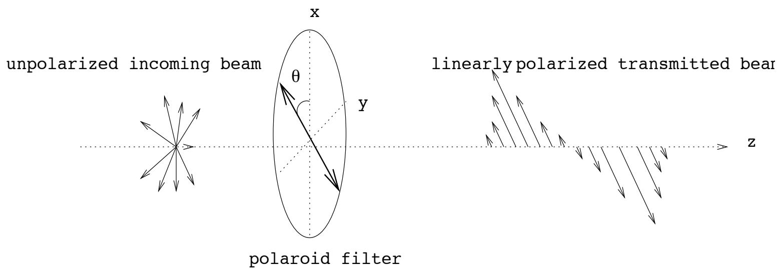
x
unpolarized incoming beam
θ
y
linearly polarized transmitted bear
z
polaroid filter

Figure 1.1 Preparation of beam polarized along θ

A convenient measure of the intensity I of the wave is given by the average of its norm, over a period $T = \frac{2\pi}{\omega}$,

$$I = \frac{1}{2}\epsilon_0 c|\mathbf{E}_0|^2 = \frac{1}{2}\epsilon_0 c E_0^2 \tag{1.4}$$

From (1.1), (1.2) it follows that the tip of the electric (and hence also magnetic) field vector describes, as a function of time, an ellipse in the (x, y) plane. There are two degenerate cases of special importance. *Linear polarization* corresponds to $\delta_x - \delta_y = m\pi$ (m integer) and the tip of the field oscillates in the (x, y) plane on a line making the angle θ with x (m even/odd). For $\theta = \frac{\pi}{4}$ (so that $\cos\theta = \sin\theta = \frac{1}{\sqrt{2}}$) and $\delta_x - \delta_y = m\frac{\pi}{2}$ (m odd integer) the polarization is left/right *circular* which means that the tip of the field rotates along a circle of radius E_0.

A light beam can be easily prepared in a state of linear polarization with the help of a filter which transmits only the component of the electric field along θ. All our subsequent discussion does not rely on a detailed explanation of the phenomenon and we do not need to know more about it[1]. Such a device is called a *polarizer* with axis θ (figure 1.1).

Analyzer-detector apparatus. Assume that a source of light has been prepared in a state of linear polarization along θ as in figure 1.1.

$$\mathbf{E}_{\text{in}}(\mathbf{x}, t) = E_0 \begin{bmatrix} \cos\theta \\ \sin\theta \\ 0 \end{bmatrix} Re\, e^{i(kz-\omega t)} \tag{1.5}$$

The intensity of the prepared beam (1.5) is proportional to E_0^2. Suppose now that this ray is transmitted through a second polarizer at an angle α. This second polarizer is called the *analyzer*. The light is then collected by a detector[2] and its

[1] In fact so-called absorptive polarizers are made of sheets of anisotropic crystals allowing electron motion preferentially in the $\theta_\perp$ direction. The $\theta_\perp$ component of the electric field sets electrons into a state of oscillation which produces the emission of an emitted anti-phase electromagnetic wave polarized along $\theta_\perp$. The later cancels the progressive $\theta_\perp$ component of the wave so that the net effect is to leave out a θ transmitted component and a $\theta_\perp$ reflected component.

[2] This can be a photoelectric cell which transforms the electromagnetic energy into a current.

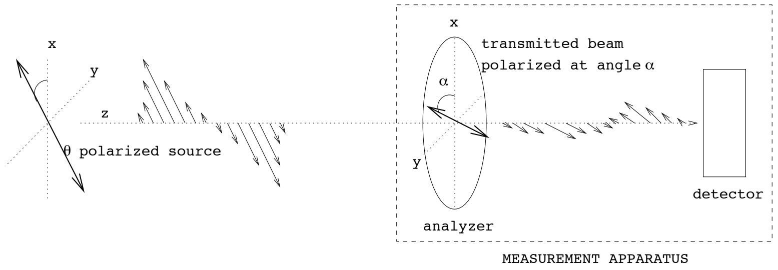

Figure 1.2 analyzer-detector measurement apparatus

intensity measured (see figure 1.2). The electric field of the final beam is obtained by projecting the incoming electric field on the analyzer axis $\mathbf{e}_\alpha$

$$\mathbf{E}_{\text{out}} = (\mathbf{E}_{\text{in}} \cdot \mathbf{e}_\alpha)\, \mathbf{e}_\alpha = E_0 \cos(\theta - \alpha) \begin{bmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{bmatrix} Re\, e^{i(kz-\omega t)} \tag{1.6}$$

and the intensity received in D is proportional to $E_0^2 \cos^2(\theta - \alpha)$. To summarize, when a beam polarized along θ is transmitted through an analyzer at an angle α, the outgoing beam is polarized along α and the fraction of intensity collected by the detector (average power per unit surface) is[3]

$$\frac{I_{\text{out}}}{I_{\text{in}}} = \cos^2(\theta - \alpha) \tag{1.7}$$

In particular if $\alpha - \theta = 0, \pi$ all the light passes through the analyzer, while if $\alpha - \theta = \pm\frac{\pi}{2}$ none of it is transmitted. The analyzer-detector system can be used as a measurement apparatus to determine the polarization of a wave (assuming we know a priori that it is linear) by adjusting the angle α such that the collected intensity varies from 0 to its maximal value. Let us now describe two simple experiments with electromagnetic waves.

Polarizing beam-splitter experiment. There exist prisms[4] that have the property of splitting a beam in two linearly polarized ones, one is polarized perpendicular to the incidence plane while the other is polarized parallel to that plane. In figure 1.3 the incidence plane is (x, z) so one ray has y polarization while the other one has x polarization. Two detectors D_x and D_y measure the outgoing intensities of each beam. Note that the polarization degree of freedom is coupled to the orbital (path of ray) degree of freedom. Before the polarizing beam-splitter the electric filed is given by (1.5) and has intensity proportional

[3] Malus law.

[4] These are made of quartz or calcite crystals whose refraction index are different for polarization perpendicular to, versus into, the incidence plane. Such crystals are called birefringent, one ray is called ordinary because the direction of refraction obeys the usual Snell law, while the other ray is called extraordinary.

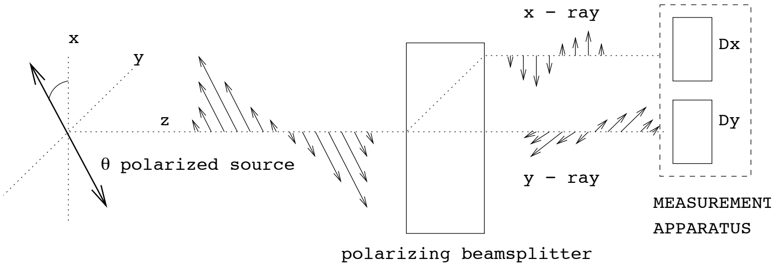

Figure 1.3 polarizing beam-splitter experiment

to E_0^2. After the beam-splitter the x-polarized ray has an electric field

$$\mathbf{E}_x = E_0 \begin{bmatrix} \cos\theta \\ 0 \\ 0 \end{bmatrix} Re\, e^{i(kz-\omega t)} \tag{1.8}$$

and the intensity detected at D_x is proportional to $E_0^2 \cos^2\theta$, while the y-polarized ray has a field

$$\mathbf{E}_y = E_0 \begin{bmatrix} 0 \\ \sin\theta \\ 0 \end{bmatrix} Re\, e^{i(kz-\omega t)} \tag{1.9}$$

and its intensity measured by D_y is proportional to $E_0^2 \sin^2\theta$. *Both detectors collect a fraction of the intensity,*

$$\frac{I_{\text{out},x}}{I_{\text{in}}} = \cos^2\theta, \qquad \frac{I_{\text{out},y}}{I_{\text{in}}} = \sin^2\theta \tag{1.10}$$

In this experiment absorption and reflection by the prism are negligible so that the sum of the these two fractions equals 1.

Decomposition-recombination experiment. Once we have decomposed light with a polarizing beam-splitter, we can recombine it with a symmetric prism. We analyze the recombined beam with an analyzer-detector apparatus (see figure 1.4). Let us carefully review the situation. Before the first beam-splitter we have *one ray* with electric field given by (1.5). The first beam-splitter splits the ray in *two parts* with electric fields given by (1.8) and (1.9). After the second beam-splitter the two rays *interfere* and the electric field of the recombined beam is the sum of (1.8) and (1.9), which equals (1.5). *The fraction of intensity collected by the analyzer-detector system is*

$$\cos^2(\theta - \alpha) \tag{1.11}$$

a fact consistent with the first experiment.

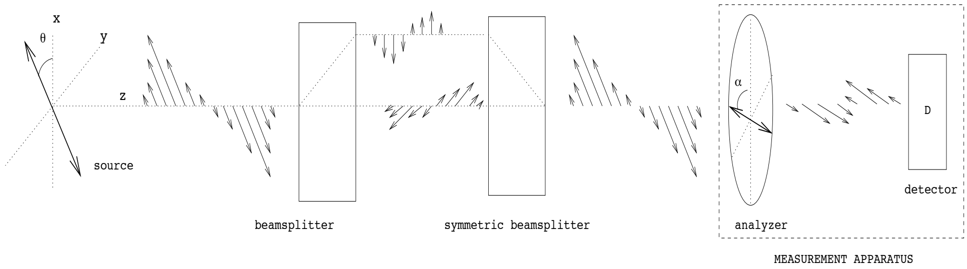

Figure 1.4 decomposition-recombination experiment

1.2 Photons

The works of Planck (1900) on the spectrum of black-body radiation, of Einstein (1905) on the photoelectric effect and Bohr (1913) on the atomic structure (and spectral lines), taught us that the interaction of light with matter occurs through discrete quanta (quantities) of energy and momentum that are absorbed and emitted. These quanta are called photons, and each photon carries an energy $\hbar\omega$ and momentum $\hbar k$ (where $\omega = ck$ still holds). If we think of the beam as a collection of independent photons, its intensity is $\hbar\omega c\frac{N}{V}$ where $\frac{N}{V}$ is the number of photons per unit volume[5]. Identifying this quantity with (1.4) we find a relation between the electric field and the number of photons associated to the electromagnetic wave.

If we diminish sufficiently the intensity of the source we arrive at a situation where in principle photons are emitted one by one. We will repeat the experiments with such a *single photon source*, that prepares them in a state of polarization θ.

Analyzer-detector apparatus. Let us first discuss how the analyzer-detector measurement apparatus works. We repeat the experiment of figure 1.2 and collect photons at the detector D. When a photon hits the detector the later clicks (an electric pulse is triggered) - we record this event as a 1, otherwise we record 0. This experiment produces a sequence

$$1001111000101010011101... \tag{1.12}$$

that looks random and where the empirical fraction of 1's is $\cos^2(\theta - \alpha)$. From this experiment we infer

$$\text{probability of detecting a photon} = \cos^2(\theta - \alpha) \tag{1.13}$$

In particular if $\alpha - \theta = 0, \pi$ all photons are detected while if $\alpha - \theta = \pm\frac{\pi}{2}$ no photon is detected.

This experiment suggests that *photons behave as particles which carry a polarization degree of freedom.* Indeed if they would behave as waves, then a part

[5] $c\frac{N}{V}$ is the number of photons per unit time per unit surface that hit a detector.

of the wave would be transmitted through the analyzer and some energy would always be measured in the detector. However *the event is discrete, the detector clicks or does not click.* Moreover *it seems impossible to predict the precise polarization outcome for each individual photon: clicks are random.* Note that the statistics of the outcomes seems to satisfy a definite formula (1.13); and this formula is the one found in the theory of electromagnetic waves (!).

The randomness of the outcome is a fundamental feature of the measurement process for quantum systems and that it is not at all obvious to reconcile this fact with our classical intuitions. One could attempt a classical interpretation[6] by saying that the photon is a particle-like object that undergoes complicated but otherwise deterministic collision processes within the analyzer, which result in a probability $\cos^2(\theta - \alpha)$ of being transmitted. Such attempts do not resist the tests of other experiments.

Let us now repeat the two previous experiments with photons that are sent one by one.

Polarizing beam-splitter experiment. Each single photon (polarized at an angle θ) goes through the prism. We observe that either D_x clicks (the upper detector register a 1 and the lower a 0) or D_y clicks (the upper detector registers a 0 and the upper a 1); but they never click simultaneously. We record two random complementary sequences with respective fractions of 1 equal to $\cos^2\theta$ and $\sin^2\theta$. Empirically,

$$\text{prob detect photon at } \mathrm{D_y} = \sin^2\theta, \qquad \text{prob detect photon at } \mathrm{D_x} = \cos^2\theta \quad (1.14)$$

The sum is equal to one which means that the photon has certainly passed through the beam-splitter.

The fact that the detectors never click simultaneously suggest as above that the *photons behave as particles.* Indeed, would they behave as waves, both detectors would collect some energy at the same time.

One may attempt the same (wrong) classical interpretation as above. A photon is a *particle*, which due to complicated but otherwise deterministic collisions with the crystal, is deflected towards the lower path with probability $\sin^2\theta$ *or* through the upper path with probability $\cos^2\theta$. This turns out to be incompatible with the next experiment.

Decomposition-recombination experiment. let us consider again the setting of figure 1.4. When photons are sent one by one we again record a sequence of random clicks, and we infer from this sequence

$$\text{prob detect photon at D} = \cos^2(\theta - \alpha) \qquad (1.15)$$

This should comes as a great surprise to the reader. Indeed this result *is not consistent with the particle-like picture of a photon, but rather with a wave-like picture*, as we now show.

[6] in the spirit of statistical mechanics, say

Theoretical prediction of the particle picture. If a photon takes the lower path in figure 1.4 its polarization is horizontal before the second beam-splitter and comes out of it in a horizontal state. Therefore the probability of transmission of such a lower-path photon through the analyzer is $\cos^2(\frac{\pi}{2} - \alpha) = \sin^2 \alpha$. Therefore

$$\text{prob(D clicks} \mid \text{lower path)} = \sin^2 \alpha \tag{1.16}$$

If the photon takes the upper path its polarization is vertical just before the second beam-splitter and comes out in a state of vertical polarization. Therefore the probability of transmission of such an upper-path photon is $\cos^2(0 - \alpha)$ and

$$\text{prob(D clicks} \mid \text{upper path)} = \cos^2 \alpha \tag{1.17}$$

Now, we have

$$\begin{aligned} \text{prob(D clicks)} =& \text{prob(D clicks} \mid \text{lower path)prob(lower path)} \\ &+ \text{prob(D clicks} \mid \text{upper path)prob(upper path)} \end{aligned} \tag{1.18}$$

Thus because of (1.14), (1.16), (1.17)

$$\text{prob detect photon at D} = \sin^2\theta \sin^2\alpha + \cos^2\theta\cos^2\alpha \tag{1.19}$$

This contradicts the experimental result (1.15) *and is therefore plain wrong !*

The term that is missing is precisely

$$2\cos\theta\cos\alpha\sin\theta\sin\alpha \tag{1.20}$$

which, in wave theory, appears because of the *interference* between the x and y components of the electric field. This suggests that a single photon follows both paths, just as a wave would do, and interferes with itself just as a wave would do

Let us summarize. We face the following situation: the decomposition experiment suggests that photons behaves in a *particle-like* manner, while he recombination experiment (1.4) suggests that photons behave in a *wave-like* fashion. As for most dilemmas, the resolution offered by *quantum theory teaches us that both pictures are two faces of a more subtle reality that goes beyond this dichotomy.* One sometimes refers to this dual behavior of light, and all known forms of matter, as the "particle-wave duality" or the "complementarity principle".

1.3 The quantum setting: first encounter

In fact all known forms of matter[7] display this particle/wave duality. As we will now see quantum mechanics offers us a picture which accommodates both behaviors and superseedes the classical pictures of wave and particle[8].

[7] For example photons, electrons, nuclei and their constituents ...

[8] According to modern physics, matter is described by relativistic quantum fields. There are underlying quantum fields (e.g. the quantum electromagnetic field, the quantum electronic

We will illustrate how the rules of quantum theory consistently explain the three experiments. The situation will be modeled in the simplest possible way which retains the basic essence of quantum mechanics.

The state of a photon is described by two degrees of freedom, an *orbital* degree of freedom and a *polarization* degree of freedom. Let us first concentrate on polarization. The state of polarization is described by a unit vector $\mathbf{e}$ perpendicular to the direction of motion. Following Dirac we call these state vectors *kets* and denote them as $|\mathbf{e}\rangle$. Since the polarization vector lies in the x, y plane it can be described in a orthonormal basis $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, corresponding to the two linear states of polarization along x and y

$$|\mathbf{e}\rangle = \lambda|\updownarrow\rangle + \mu|\leftrightarrow\rangle, \qquad |\lambda|^{\mathbf{2}} + |\mu|^{\mathbf{2}} = \mathbf{1} \tag{1.21}$$

Here λ and μ are complex numbers. thus a general polarization state is a normalized two component vector belonging to $\mathbf{C}^2$. The space $\mathbf{C}^2$ is our first and simplest example of a space of quantum states.

A state of linear polarization along θ corresponds to $\lambda = \cos\theta$ and $\mu = \sin\theta$, so that (1.21) becomes

$$|\theta\rangle = \cos\theta|\updownarrow\rangle + \sin\theta|\leftrightarrow\rangle \tag{1.22}$$

On the other hand for circular polarization the x and y components of the polarization vector have a $\frac{\pi}{2}$- phase difference. Two basis states with circular polarization are,

$$|L/R\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle \pm i|\leftrightarrow\rangle) \tag{1.23}$$

Given a state vector $|\Phi\rangle$ its *adjoint* (also called hermitian conjugate) is obtained by taking the complex conjugate and transposing $\overline{|\Phi\rangle}^T$. This is denoted as a *bra*

$$\langle\Phi| = \overline{|\Phi\rangle}^T \tag{1.24}$$

The usual inner product (defined over a complex vector space) is called the *bracket*

$$\langle\Psi|\Phi\rangle = (\overline{|\Psi\rangle}^T) \cdot (|\Phi\rangle) \tag{1.25}$$

As an example consider the inner product between two polarization state vectors. First the conjugate of a linearly polarized state is

$$\langle\alpha| = \langle\updownarrow|\cos\alpha + \langle\leftrightarrow|\sin\alpha \tag{1.26}$$

The inner product with $|\theta\rangle$ then is

$$\begin{aligned}\langle\alpha \mid \theta\rangle &= (\langle\updownarrow|\cos\alpha + \langle\leftrightarrow|\sin\alpha) \cdot (\cos\theta|\updownarrow\rangle + \sin\theta|\leftrightarrow\rangle)\\ &= \cos\alpha\cos\theta + \sin\alpha\sin\theta\\ &= \cos(\theta-\alpha) \end{aligned}\tag{1.27}$$

field, the quark field etc...) which may manifest themselves in a wave-like or particle-like fashion depending on the situation. We will not introduce field theoretical notions in this course.

To obtain the second equality one expands the braces into four terms, uses linearity of the bracket and the orthonormality condition,

$$\langle p \mid p' \rangle = \delta_{pp'} \tag{1.28}$$

This trivial calculation has been done in the linear polarization orthonormal basis $\{| \leftrightarrow\rangle, | \updownarrow\rangle\}$. It is instructive to check that the circularly polarized states $\{|L\rangle, |R\rangle\}$ form another orthonormal basis of the two dimensional complex vector space.

Let us now introduce the orbital degree of freedom in the picture. For a freely moving photon, i.e a photon that does not interact with a material object, the orbital state is entirely described once we know its *momentum* $\mathbf{k}$, which has a *direction* $\mathbf{k}/k$ and a *norm* $k = \frac{\omega}{c}$. The state vector is now denoted as $|\mathbf{k}, \mathbf{e}\rangle$. This state freely evolves with time and for a photon of frequency ω the time evolution simply amounts to a multiplicative phase factor, which does not change the momentum and the polarization. The photon state at time t is

$$|\Psi_{\mathbf{k},\mathbf{e}}(t)\rangle = e^{-i\omega t}|\mathbf{k}, \mathbf{e}\rangle \tag{1.29}$$

An explanation is in order here about the kets indexed by two degrees of freedom. We will see in the next chapter that the mathematical rule to combine degrees of freedom is the tensor product; this means that $|\mathbf{k}, \mathbf{e}\rangle = |\mathbf{k}\rangle \otimes |\mathbf{e}\rangle$ and that the inner product is

$$\langle \mathbf{k}', \mathbf{e}' \mid \mathbf{k}, \mathbf{e}\rangle = \langle \mathbf{k}' \mid \mathbf{k}\rangle \cdot \langle \mathbf{e}' \mid \mathbf{e}\rangle \tag{1.30}$$

Finally the momentum vectors themselves form an orthonormal basis $\langle \mathbf{k}' \mid \mathbf{k}\rangle = \delta_{\mathbf{k}',\mathbf{k}}$.

As we will see in the next chapter, in general, the time-evolution of isolated systems is given by a unitary transformation. In (1.29) the unitary transformation is simply the multiplication by the phase factor. When the photon interacts with matter (for example with the analyzer, the beam-splitter) one has in principle to describe the unitary evolution of the total system (photon + analyzer or photon + beam-splitter), which is then more complicated. Here we do not have to discuss such issues as we consider only the in-going and out-going states which are those of freely moving photons.

When we make a measurement on a system, the system that is observed cannot be considered as isolated and the state is modified in a non-unitary way. Explaining the measurement process is a subject that has been (and sometimes is still) much debated since the early days of quantum mechanics. An operational rule, to determine the outcome of a measurement is given by the so-called *measurement postulate* (Born, Heisenberg, Bohr 1924-1927) in the form advocated

ψ
MEASUREMENT APPARATUS
φ

Figure 1.5 measurement with initial state $|\Psi\rangle$ and outcome $|\Phi\rangle$.

by what has been named the Copenhagen School[9] (figure 1.5). Here we give it in a rough form, and will be more precise in the next chapter.

If a system is initially prepared in the state $|\Psi\rangle$ and the outcome of the measurement is a state $|\Phi\rangle$, the probability of the transition $|\Psi\rangle \to |\Phi\rangle$ is

$$\text{Prob}(|\Psi\rangle \to |\Phi\rangle) = |\langle \Phi \mid \Psi \rangle|^2 \tag{1.31}$$

One cannot predict the outcome of the transition but only its frequency of occurrence during repeated identical experiments with identical initial states.

The transition between the initial and final state is also called "reduction" or "collapse" of the state. In a more precise formulation of the measurement postulate, in the next chapter, we will see that the transition probabilities of all possible outcomes sum to one.

The re-interpretation of the experiments in the next section should make this rather abstract postulate a bit more "natural".

1.4 Quantum interpretation of experiments.

Analyzer-detector apparatus. We assume that the source prepares single photons in the linearly polarized, freely moving state

$$|\Psi_{\mathbf{k},\theta}(t)\rangle = e^{-i\omega t}|\mathbf{k}, \theta\rangle \tag{1.32}$$

If the measurement apparatus is the analyzer-detector system of figure 1.2, the measurement postulate tells us that the probability to find the photon in state $|\mathbf{k}, \alpha\rangle$ is

$$|\langle \mathbf{k}, \alpha \mid \Psi_{\mathbf{k},\theta}(t)\rangle|^2 = |\langle \alpha \mid \theta \rangle|^2 = \cos^2(\theta - \alpha) \tag{1.33}$$

This is consistent with the experimentally measured frequency of clicks in D.

Polarizing beam-splitter experiment. Before the beam-splitter the photon

[9] Einstein never agreed that this rule is the final story. In his words "I, at any rate, am convinced that He (God) does not throw dice". Bohr replied "Einstein, don't tell God what to do". In any case, this rule has not been challenged by experiment so far, and there is hardly any more satisfying theoretical framework to date. In this course we stick to this rule !

state is (1.32), which is equal to

$$e^{-i\omega t}(\cos\theta|\mathbf{k},\updownarrow\rangle + \sin\theta|\mathbf{k},\leftrightarrow\rangle) \tag{1.34}$$

After the beam-splitter it becomes

$$e^{-i\omega t}(\cos\theta|\mathbf{k}_u,\updownarrow\rangle + \sin\theta|\mathbf{k}_l,\leftrightarrow\rangle) \tag{1.35}$$

where $\mathbf{k}_u$ and $\mathbf{k}_l$ label the upper and lower paths[10]. Notice that contrary to (1.34), in (1.35) we cannot separate the orbital and polarization degrees of freedom into a tensor product: it can be shown that for (1.35) this is an intrinsic property that does not depend on the basis. We say that the orbital and polarization degrees of freedom have been *entangled* by the beam-splitter. Entangled states depart fundamentally from the classical picture and retain quantum correlations that are missing in the classical interpretation. As we will see in this course they play a very important role in quantum information and computation because they may offer resources that are non-classical.

Now we consider the two detectors as our measurement apparatus. The measurement postulate tells us that the probability to observe the photon in state $|\mathbf{k_u},\updownarrow\rangle$ is

$$|\langle\mathbf{k_u},\updownarrow|\; e^{-i\omega t}(\cos\theta|\mathbf{k}_u,\updownarrow\rangle + \sin\theta|\mathbf{k}_l,\leftrightarrow\rangle)|^2 = \cos^2\theta \tag{1.36}$$

Similarly the probability to observe it in the state $|\mathbf{k}_l,\leftrightarrow\rangle$ is

$$|\langle\mathbf{k}_l,\leftrightarrow|\; e^{-i\omega t}(\cos\theta|\mathbf{k}_u,\updownarrow\rangle + \sin\theta|\mathbf{k}_l,\leftrightarrow\rangle)|^2 = \sin^2\theta \tag{1.37}$$

This is consistent with the experimental fractions of clicks at D_x and D_y.

Recombination experiment. The second polarizing beam-splitter transforms the entangled state (1.35) back to (1.32). The later state enters the measurement apparatus constituted by the analyzer-detector system. Therefore the probability of observing $|\mathbf{k},\alpha\rangle$ is simply given by (1.33). This is the experimental frequency of clicks at D ! The quantum interpretation does not loose track of the interference term (1.20).

1.5 Notion of quantum bit

There exist many quantum systems in nature that can be described by state vectors which belong to the vector space $\mathbf{C}^2$, the two dimensional complex vector space. If we call $|0\rangle$ and $|1\rangle$ two orthonormal basis states a general state vector takes the form

$$|\psi\rangle = \lambda|0\rangle + \mu|1\rangle, \qquad |\lambda|^2 + |\mu|^2 = 1 \tag{1.38}$$

[10] Here we may imagine that the paths are not quite in the same direction so that these two labels are different. In principle one should make a more complete description of the orbital part of the state that takes into account the finite width of the beams.

It will often be convenient to identify

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1.39}$$

and

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.40}$$

and in quantum information theory it is customary to call this canonical basis the *computational basis.* Of course one can represent the quantum bit $|\psi\rangle$ in any other basis, and one that we will often use one that is obtained by a standard 45 degree real rotation

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.41}$$

This basis will be called the Hadamard basis. Since the vector space is complex we can make more general unitary transformations. For example

$$|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \qquad |R\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \tag{1.42}$$

We have already seen a physical realization of a quantum bit, namely the photon polarization. If we identify the computational basis with horizontal/vertical polarized photon states, then the Hadamard basis corresponds to polarized states at 45 degree angle, and the last basis obtained by a unitary transformation is physically realized by circularly left/right polarized photons. A physically meaningful parametrization of general polarization state is

$$|\psi\rangle = e^{i\delta_x} \cos\theta | \updownarrow\rangle + e^{i\delta_y} \sin\theta | \leftrightarrow\rangle \tag{1.43}$$

If we rotate our reference frame (around z) by angle β, then the state vector is obtained from the above expression by $\theta \to \theta - \beta$. In particular if the reference frame is rotated by 2π we recover the same state vector. These states form ratgher trivial representations of the group of two-dimensional rotations (about the z-axis say).

Another very common but physically different quantum bit is the *spin* $\frac{1}{2}$. The most famous elementary particle (of obvious importance in our everyday life since it transports electricity, interacts with sunlight ...) that has spin $\frac{1}{2}$ is the electron[11]. There exist also many composite systems, such as nuclei or atoms that carry a total spin of $\frac{1}{2}$. A very rough intuitive way of thinking about spin is to view the particle (the electron say) as having intrinsic spinning motion. If the particle spins about the z axis, its spin is (pointing) $|\uparrow\rangle$ or $|\downarrow\rangle$ according to its direction of rotation. These two states form a basis and the most general spin state is

$$|\psi\rangle = \lambda|\uparrow\rangle + \mu|\downarrow\rangle, \qquad |\lambda|^2 + |\mu|^2 = 1 \tag{1.44}$$

[11] Constituents of nuclei, protons and neutrons also have spin $\frac{1}{2}$. In particular the interaction of the nuclear spins with magnetic fields is at the basis of Nuclear Magnetic Resonance, used for example in medical imaging.

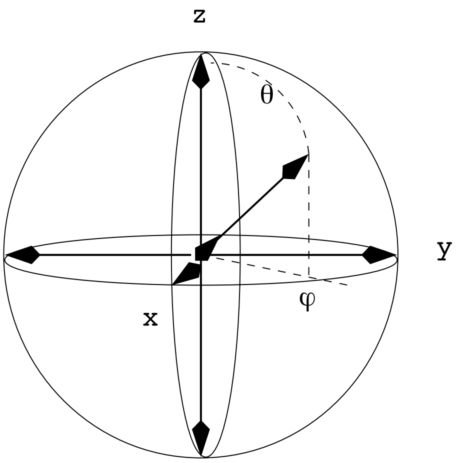

Figure 1.6 Bloch sphere. Computational (z), Hadamard (x), circular (y) basis states

Spin $\frac{1}{2}$ states are two dimensional (complex) representations of the group of rotations in three dimensions. A meaningful parametrization of the states is

$$|\psi\rangle = e^{i\frac{\phi}{2}} \cos\frac{\theta}{2}|\uparrow\rangle + e^{-i\frac{\phi}{2}} \sin\frac{\theta}{2}|\downarrow\rangle \tag{1.45}$$

These states can be represented by the tip of a vector on the *Bloch sphere* (figure 1.6) with the usual spherical coordinates (θ, ϕ). We have the following correspondence (up to phase factors):

$$\theta = 0,\ \pi \qquad |\uparrow\rangle, |\downarrow\rangle, \qquad \text{particle spin along z} \tag{1.46}$$

$$\theta = \frac{\pi}{2}, \phi = 0,\ \pi \qquad |\uparrow\rangle \pm |\downarrow\rangle, \qquad \text{particle spin along x} \tag{1.47}$$

$$\theta = \frac{\pi}{2}, \phi = \pm\frac{\pi}{2} \qquad |\uparrow\rangle \pm i|\downarrow\rangle, \qquad \text{particle spin along y} \tag{1.48}$$

The polarization and spin $\frac{1}{2}$ quantum bits are different representations of the rotation group in quantum mechanics (ultimately coming from the representations of the Lorentz group of relativity).

There exist also other realizations of the quantum bit that have nothing to do with the representations of the rotation group. An example is given by the benzene molecule C_6H_6 that can be in the two states that differ in the arrangement of single and double electronic bonds (figure 1.7). But the molecule can also be found in a *resonating state* such as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \tag{1.49}$$

What is the difference between a classical bit and a quantum bit ? A classical bit is an abstraction of a physical quantity that can be reasonably well described

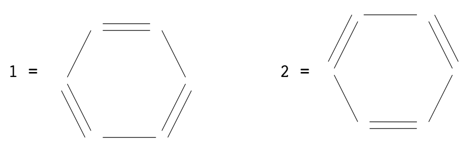

Figure 1.7 possible arrangements of chemical bonds

by a two valued quantity. Examples are the charge in a capacitor, a voltage difference, or the magnetization of a Weiss domain. Classical information theory is sufficiently universal so that it does not have to account for the detailed physical properties of the classical bits. The only underlying assumption is that these exist in two definite values 0 or 1 (let us pretend that noise is absent). Suppose a classical bit is given to you and that you have no information whatsoever about its value. To gain information about its value you can observe it (measure the charge, the voltage difference) and its value is then discovered. By *discovered* we mean that it already had the observed value before the measurement, and that the measurement has not destroyed it.

A quantum bit is also an abstraction of physical as the above examples have shown. It is well described by a two dimensional complex vector. In the same spirit than in the classical case, quantum information theory is sufficiently universal so that many of its aspects are independent of the concrete physical realization. However the important point is that it takes into account the general underlying laws of quantum mechanics. This means in particular that extracting information from quantum bits is quite different than in the classical case. Suppose that a quantum bit is given to you in some state $|\psi\rangle$ on which you do not have any information whatsoever. In order to determine $|\psi\rangle$, we have to observe it (agree ?). To perform a measurement we have to select an apparatus, in other words an orthonormal basis $\{|b_1\rangle, |b_2\rangle\}$. The measurement process then reduces the quantum bit to $|b_1\rangle$ or to $|b_2\rangle$. So we have lost the original state (forever) and have not gained any knowledge (of the initial state) because the final state depends on *our own* choice of basis. Note however that if we are given many copies of $|\psi\rangle$ we can measure all of them in the same basis and get a hold of the probabilities $|\langle b_1 \mid \psi\rangle|^2$, $|\langle b_2 \mid \psi\rangle|^2$.

1.6 A random number generator

At this point the reader may well wonder if quantum laws offer any useful resource in order to process information. In this course we will see that this is so. Here we illustrate this with a very simplified model for a random number generator.

A source sends a beam of photons on a semi-transparent mirror (figure 1.8). The later splits the beam in two parts, the transmitted and reflected beams. If the source is classical we observe that the two detectors each collect a fraction of

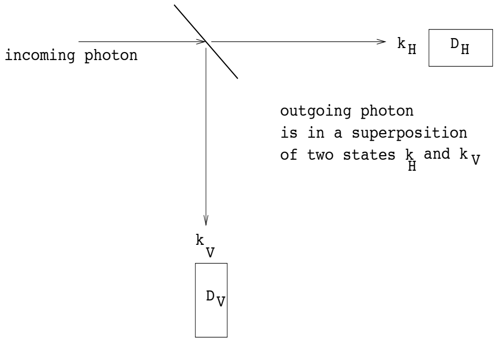

Figure 1.8 semi-transparent mirror

the incoming intensity of the beam. Assuming that the semi-transparent mirror is perfect each detector collects half of the intensity.

When the intensity of our source is lowered sufficiently so that it becomes a single photon source. Photons go through the mirror one at a time, we observe that *either* D_H *or* D_V clicks, never the two at the same time. We obtain a sequence of clicks 0100011101010101000110111100 that looks Bernoulli with parameter $p = \frac{1}{2}$.

The interpretation of this experimental setup, in the framework of quantum mechanics, is as follows. We drop the polarization index as it plays no role here. A single photon is incoming in the semi-transparent mirror and the state of the photon after the mirror is,

$$e^{i\omega t}\frac{1}{\sqrt{2}}(|\mathbf{k}_H\rangle + |\mathbf{k}_V\rangle) \tag{1.50}$$

This state is a superposition. The outcome of the measurement by the detectors cannot be predicted. The probability that the photon is observed in state $|\mathbf{k}_H\rangle$ is

$$|\langle\mathbf{k}_H \mid e^{i\omega t}\frac{1}{\sqrt{2}}(|\mathbf{k}_H\rangle + |\mathbf{k}_V\rangle)|^2 = \frac{1}{2} \tag{1.51}$$

and similarly the probability that it is observed in state $\mathbf{k}_V$ is

$$|\langle\mathbf{k}_V \mid e^{i\omega t}\frac{1}{\sqrt{2}}(|\mathbf{k}_H\rangle + |\mathbf{k}_V\rangle)|^2 = \frac{1}{2} \tag{1.52}$$

So the measurement process produces a perfectly random sequence.

What do we mean by ”perfectly random sequence”? Of course, the sequence is perfectly random only in principle, because in the real experiment there are imperfections, for example, the source is only approximately a single photon source and the semi-transparent mirror has a small bias etc.... But the point here is that, according to the standard interpretation of quantum mechanics, the measurement process produces ”true randomness” and not ”pseudo-randomness”: the clicks are not the result of some underlying deterministic process. This point

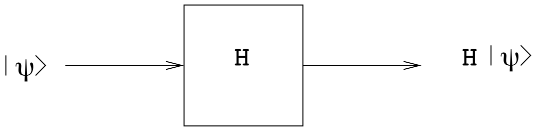

Figure 1.9 Hadamard gate as a model for a semi-transparent mirror

has been much debated by the founding fathers of 20-th century physics and notably by Einstein and Bohr. According to Einstein "God does not play dice", a view that Bohr dismissed. Until today, no other theoretical framework has, successfully described as many phenomena as quantum theory does, and we have so far no experiment that forces us to abandon the standard quantum framework. It is in this sense that we declare the sequence perfectly random.

A slightly more abstract representation in quantum information theory language of this experiment is depicted on figure 1.9. We prepare and measure states in the computational basis $|0\rangle, |1\rangle$. The initial state $|0\rangle$ goes through a Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1.53}$$

which produces the state

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.54}$$

When we perform a measurement on this state the outcome is $|0\rangle$ with probability

$$|\langle 0|H|0\rangle|^2 = \frac{1}{2} \tag{1.55}$$

or $|1\rangle$ with probability

$$|\langle 1|H|0\rangle|^2 = \frac{1}{2} \tag{1.56}$$

We note that quantum random number generators based on these principles have been realized and are even commercialized. See for example http://www.idquantique.com/true-random-number-generator/products-overview.html

2 Mathematical formalism of quantum mechanics

Quantum mechanics is the best theory that we have to explain the physical phenomena (if we exclude gravity). The elaboration of the theory has been guided by experimental discoveries, as well as thought experiments and conceptual ideas of a great generation of physicist. Milestones of the development of quantum theory are from 1900 to 1930 are: Planck on black body spectrum (1900), Einstein on the photon (1905), Bohr on the atom (1913), De Broglie on the wave function (1924), Schroedinger on the wave function evolution (1926), Born on the interpretation of the wave function (1926), Heisenberg on matrix mechanics (1925), Dirac on relativistic QM (1930). Some never completely accepted their own ideas, although these still form the best theory that we have today. The mathematical form of the theory that we find in textbooks has been put forward by Dirac and von Neumann in the 30's Since then the quantum laws of physics have been used unchanged[1] to successfully describe an impressive range of phenomena ranging from macroscopic solid state, molecular to atomic, nuclear, sub-nuclear and particle physics scales.

The arena of QM is Hilbert space so we begin with some mathematical reminders on linear algebra in such spaces. Our goal is also to carefully introduce the reader to Dirac's bra and ket notation. Then we introduce 5 basic principles that define QM. We also discuss two genuine quantum notions, namely, entangled states and the no-cloning theorem.

2.1 Linear algebra in Dirac notation

A *Hilbert space* $\mathcal{H}$ is a vector space over the field of complex numbers $\mathbf{C}$, with an inner product. For a finite dimensional Hilbert space that is all. For an infinite dimensional Hilbert space we require that it is complete and separable[2]. In quantum information theory we will almost always deal with Hilbert spaces of quantum bits which are discrete by nature, hence our Hilbert spaces are finite dimensional and we do not have to worry about completeness and separability.

The vectors will be denoted $|\psi\rangle$ (pronounced ket psi). The hermitian conjugate

[1] Combined with special relativity when needed

[2] Complete means that all Cauchy sequences converge in the norm induced by the inner product and separable that there is a contable orthonormal basis.

(transpose and complex conjugate) is denoted by $\langle\psi|$ (pronounced bra psi). The inner product is denoted $\langle\phi|\psi\rangle$. This is the inner product of the vectors $|\phi\rangle$ and $|\psi\rangle$ and is called a *bracket* (for bra-ket). The inner product must satisfy:

1. *Positivity*: $\langle\phi|\phi\rangle \geq 0$ with equality if and only if $|\phi\rangle = 0$.
2. *Linearity*: $\langle\phi|(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha\langle\phi|\psi_1\rangle + \beta\langle\phi|\psi_2\rangle$, $\alpha, \beta \in \mathbf{C}$
3. *Skew symmetry*: $\langle\phi|\psi\rangle = \overline{\langle\psi|\phi\rangle}$ where the bar denotes complex conjugation.

A ray is an equivalence class of vectors of the form $\lambda|\psi\rangle$ where $\lambda \in \mathbf{C}$ and $|\psi\rangle$ is a specified vector. This specified vector is a representative of the ray.

Example 1: Qbit or two level system. $\mathcal{H} = \mathbf{C}^2 = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \text{ with } \alpha, \beta \in \mathbf{C} \right\}$. The inner product is $(\overline{\gamma}, \overline{\delta}) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \overline{\gamma}\alpha + \overline{\delta}\beta$. In Dirac notation we have

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Moreover

$$(\overline{\gamma}, \overline{\delta}) = \overline{\gamma}\langle 0| + \overline{\delta}\langle 1|$$

and

$$(\overline{\gamma}\langle 0| + \overline{\delta}\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \overline{\gamma}\alpha\langle 0|0\rangle + \overline{\gamma}\beta\langle 0|1\rangle + \overline{\delta}\alpha\langle 1|0\rangle + \overline{\delta}\beta\langle 1|1\rangle = \overline{\gamma}\alpha + \overline{\delta}\beta$$

Example 2: particle in three dimensional space. $\mathcal{H} = L^2(\mathbf{R}^3) = \{f : \mathbf{R}^3 \to \mathbf{C}, \int d^3x|f(x)|^2 < \infty\}$. The inner product is $\langle f|g\rangle = \int d^3x\overline{f(x)}g(x)$ and the induced norm $||f||_2 = \langle f|f\rangle^{1/2} = \int d^3x|f(x)|^2$. This space plays a fundamental role in quantum mechanics but we will not need it in this course, since we deal only with discrete degrees of freedom.

We will need the notion of *tensor product.* Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces with two finite basis. Let the basis of the first space be $|i\rangle_1$, $i = 1, ..., n_1$, $\dim \mathcal{H}_1 = n_1$ and that of the second space $|j\rangle_2$, $j = 1, ..., n_2$, $\dim \mathcal{H}_2 = n_2$. We can form the tensor product space

$$\mathcal{H}_1 \otimes \mathcal{H}_2$$

which is simply the new Hilbert space spanned by the basis vectors

$$|i\rangle_1 \otimes |j\rangle_2$$

(also denoted $|i, j\rangle$ or $|i\rangle_1|j\rangle_2$). There are $n_1 n_2$ such vectors so

$$\dim \mathcal{H}_1 \otimes \mathcal{H}_2 = n_1 n_2$$

A general element of the tensor product space is of the form

$$|\psi\rangle = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} c_{ij}|i,j\rangle = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} c_{ij}|i\rangle_1 \otimes |j\rangle_2$$

Lastly we have to say what is the inner product in the product space:

$$\langle i',j'|i,j\rangle = (\langle i'|_1 \otimes \langle j'|_2)(|i\rangle_1 \otimes |j\rangle_2) = \langle i'|i\rangle_1 \langle j'|j\rangle_2$$

Example 3. For one Qbit the Hilbert space is $\mathbf{C}^2$. We will see that the Hilbert space of two Qbits is $\mathbf{C}^2 \otimes \mathbf{C}^2$. The basis vectors of $\mathbf{C}^2 \otimes \mathbf{C}^2$ are $\{|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle\}$ or $\{|0,0\rangle$, $|0,1\rangle$, $|1,0\rangle$, $|1,1\rangle\}$. A general state is

$$|\psi\rangle = \alpha_{00}|0,0\rangle + \alpha_{01}|0,0\rangle + \alpha_{10}|0,0\rangle + \alpha_{11}|1,1\rangle$$

We have $\dim \mathbf{C}^2 \otimes \mathbf{C}^2 = 4$ and of course $\mathbf{C}^2 \otimes \mathbf{C}^2$ is isomorphic to $\mathbf{C}^4$: However it is important to stress that in QM the meaning of the first representation is really that *two Qbits are involved* : in general it is too difficult (meaningless in some sense) to do physics in a bad representation. Here a few inner products are $\langle 0,0|0,0\rangle = \langle 0|0\rangle\langle 0|0\rangle = 1$, $\langle 0,1|0,1\rangle = \langle 0|0\rangle\langle 1|1\rangle = 1$, $\langle 0,1|1,1\rangle = \langle 0|1\rangle\langle 1|1\rangle = 0$ etc... From these one can compute the inner product of $|\psi\rangle$ and $|\phi\rangle = \beta_{00}|0,0\rangle + \beta_{01}|0,0\rangle + \beta_{10}|0,0\rangle + \beta_{11}|1,1\rangle$. We find the natural product of $\mathbf{C}^4$, $\langle\phi|\psi\rangle = \overline{\beta}_{00}\alpha_{00} + \overline{\beta}_{01}\alpha_{01} + \overline{\beta}_{10}\alpha_{10} + \overline{\beta}_{11}\alpha_{11}$. It is often useful to work in the canonical basis of $\mathbf{C}^4$

$$\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix} = |0,0\rangle \quad \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix} = |0,1\rangle \quad \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix} = |1,0\rangle \quad \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix} = |1,1\rangle$$

Once this (conventional) correspondence is fixed we can infer the rules for tensoring vectors in their coordinate representation

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \qquad \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$\begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \qquad \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

You can see that in this course the convention is that you multiply the first set of coordinates by the second vector . All these rules generalize to $\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^2$ etc...

Cauchy-Schwarz inequality. As usual:

$$|\langle\phi|\psi\rangle| \leq \langle\phi|\phi\rangle^{1/2}\langle\psi|\psi\rangle^{1/2}$$

Closure relation. Let $|i\rangle$, $i = 1, ..., n$ be an orthonormal basis of the n-dimensional Hilbert space. Any vector $|\phi\rangle$ can be expanded as

$$|\phi\rangle = \sum_{i=1}^{n} c_i|i\rangle, \qquad c_i = \langle i|\phi\rangle$$

where the components c_i are obtained by projecting $|\phi\rangle$ over the basis vectors. The above expansion can be rewritten as

$$|\phi\rangle = \sum_{i=1}^{n} |i\rangle\langle i|\phi\rangle$$

Note that $|i\rangle\langle i|$ is the projection operator on vector $|i\rangle$. We can view $\sum_{i=1}^{n} |i\rangle\langle i|$ as the identity operator acting on $|\phi\rangle$, thus we have the *closure relation*

$$\sum_{i=1}^{n} |i\rangle\langle i| = I$$

This turns out to be a very useful identity for doing practical calculations in Dirac notation. Note that this identity is simply the spectral decomposition of the identity.

Observables. In QM observable quantities are represented by linear operators (matrices) on $\mathcal{H}$. Let us briefly review a few important facts. The map $A : \mathcal{H} \to \mathcal{H}$, $|\psi\rangle \to A|\psi\rangle$ is linear if

$$A(\alpha|\phi_1\rangle + \beta|\phi_2\rangle) = \alpha(A|\phi_1\rangle) + \beta(A|\phi_2\rangle)$$

The matrix elements of A in a basis $\{|i\rangle, i = 1, ..., n\}$ of $\mathcal{H}$ are denoted by $\langle i|A|j\rangle$ or A_{ij}. Given A, the *adjoint* of A is denoted $A^\dagger$ and defined by

$$\langle\phi|A^\dagger|\psi\rangle = \overline{\langle\psi|A|\phi\rangle}$$

So the adjoint (or hermitian conjugate) is the operator which has transposed and conjugate matrix elements. We say that A is self-adjoint (or hermitian) if $A = A^\dagger$. The later type of operators play a very central role in QM because observable quantities are represented by self-adjoint operators: the reader can guess that this must be so because any physical measurement is expressed by a real number (why ?) and self-adjoint operators have real eigenvalues. The reader can check that $(A + B)^\dagger = A^\dagger + B^\dagger$ and $(AB)^\dagger = B^\dagger A^\dagger$.

We will also need the following notations for the *commutator*

$$[A, B] = AB - BA$$

and the anticommutator

$$\{A, B\} = AB + BA$$

Projectors in Dirac notation. The linear operator $|i\rangle\langle i| = P_i$ is the projector on the basis vector $|i\rangle$. To check that P_i is a projector we need to verify that $P_i^\dagger = P_i$ and $P_i^2 = P_i$. Here is how one does it in Dirac notation

$$P_i^\dagger = (|i\rangle\langle i|)^\dagger = (\langle i|)^\dagger(|i\rangle)^\dagger = |i\rangle\langle i| = P_i$$

$$P_i^2 = (|i\rangle\langle i|)(|i\rangle\langle i|) = |i\rangle\langle i|i\rangle\langle i| = |i\rangle\langle i| = P_i$$

Since $|i\rangle$ and $|j\rangle$ are orthogonal for $i \neq j$ we have $P_iP_j = P_jP_i = 0$. Indeed

$$P_iP_j(|i\rangle\langle i|)(|j\rangle)(\langle j|) = |i\rangle\langle i|j\rangle\langle j|) = 0$$

$$P_jP_i(|j\rangle\langle j|)(|i\rangle\langle i|) = |j\rangle\langle j|i\rangle\langle i|) = 0$$

Note that if $|\phi\rangle$ is any vector of the Hilbert space, then $P_\phi = |\phi\rangle\langle\phi|$ is the projector on $|\phi\rangle$.

Spectral decomposition. Hermitian operators (matrices) on a Hilbert space have a *spectral decomposition* or *spectral representation*,

$$A = \sum_n a_n P_n$$

where $a_n \in \mathbf{R}$ are the eigenvalues and P_n the eigenprojectors of A. The eigenspaces of A are spanned by the orthonormal eigenvectors $|\phi_{nj}\rangle$ associated to the eigenvalue a_n:

$$A|\phi_{nj}\rangle = a_n|\phi_{nj}\rangle, \quad P_n = \sum_j |\phi_{nj}\rangle\langle\phi_{nj}|$$

The index j takes into account the possible degeneracy of a_n. From the orthonormality of the eigenvectors one sees that $P_nP_m = P_mP_n = 0$ for $n \neq m$. Note that for given n one always has the liberty to rotate the basis $\{|\phi_{nj}\rangle\}$ in the subspace of P_n. Moreover we have the closure relation

$$I = \sum_n P_n = \sum_{n,j} |\phi_{n,j}\rangle\langle\phi_{nj}|$$

We will often write the spectral decomposition as

$$A = \sum_{n,j} a_n|\phi_{nj}\rangle\langle\phi_{nj}|$$

In the non-degenerate case this becomes simply $A = \sum_n a_n|\phi_n\rangle\langle\phi_n|$.

2.2 Principles of quantum mechanics

In this paragraph we explain the 5 basic principles of QM. In a nutshell:

- isolated systems are described by *states of a Hilbert space*,
- they *evolve unitarily with time*,
- *observable* quantities are described by *hermitian matrices*,

- measurement is a *distinct process* from time evolution: it is a *random projection*,
- systems can be brought together and *composed*: their Hilbert space is a tensor product space.

Their meaning, interpretation and soundness has been debated over the first half of the 20-th century by the founding fathers of QM and by their followers, specially the measurement postulate.

Principle 1: states. The state of a quantum system - that is isolated from the rest of the universe - is *completely* described by a ray in a Hilbert space. We require that the representative vector $|\psi\rangle \in \mathcal{H}$ is normalized to one, $\langle\psi|\psi\rangle = 1$.

Example 4.

- To describe the polarization of the photon we take $\mathcal{H} = \mathbf{C}^2$. States are vectors in $\mathbf{C}^2$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. For a linearly polarized state $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, for a circularly polarized state $|\tilde{\theta}\rangle = \cos\theta|0\rangle + i\sin\theta|1\rangle$, and for elliptic polarization $\cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$.
- The spin $\frac{1}{2}$ of an electron (say) is described by the same Hilbert space.
- For a Benzene molecule the Hilbert space is again the same and is spanned by the two valence bond states (see chapter 1):

$$|\psi\rangle = \alpha|1\rangle + \beta|2\rangle$$

- For a particle in $\mathbf{R}^3$ we have $\mathcal{H} = L^2(\mathbf{R}^3)$ as explained before. These are called wave functions and are normalized $\int d^3x|\psi(x)|^2 = 1$.

Remark. If $|\psi\rangle$ is a description of a system then $e^{i\lambda}|\psi\rangle$ is an equally good description. The *global* phase $\lambda \in \mathbf{R}$ is not an observable quantity and can be fixed arbitrarily. This is why QM states should really be defined as rays. However the *relative* phase of states is observable through interference effects. You might also wonder what is the difference between spin one-half and photon polarization. In fact photon polarization states and spin one-half states behave very differently under spatial rotations of the coordinate system (or the lab). Under a rotation of the reference frame the state of polarization of a photon behaves like a vector. In particular under a 2π rotation we recover the same state. On the other hand for spin one-half behaves as a spinor (sometimes called half-vector) under a rotation of the reference frame. In particular, under a 2π rotation we recover the opposite state. In QM the representations of the rotation group (and any other group) on the Hilbert space does not have to satisfy $\mathbf{R}(2\pi) = 1$, precisely because states are rays. Therefore a phase is allowed for $\mathbf{R}(2\pi)|\psi\rangle = e^{i\lambda}|\psi\rangle$. All these aspects of QM will not mater too much in this course so we omit more explanations on what "spin" and "photon polarization" really are. A more profound discussion of these aspects would require to explain the representation theory of the Lorentz group of special relativity.

Principle 2: time evolution. An isolated quantum system evolves with time in a unitary fashion. This means that if $|\psi\rangle$ is the state at time 0, the state at time t is of the form $U_t|\psi\rangle$ where U_t is a unitary operator from $\mathcal{H} \to \mathcal{H}$. Here unitary means that $U_t^\dagger U_t = U_t U_t^\dagger = 1$ or equivalently $U_t^{-1} = U_t^\dagger$.

Unitary time evolution forms a group (it is a representation of translations along the time axis) in the sense that

$$U_{t=0} = I, \qquad U_{t_1} U_{t_2} = U_{t_1+t_2}$$

QM tells us how to compute U_t for a given system: one has to solve the *Schroedinger equation* or the *Heisenberg equations of motion*. These are equivalent in fact. The first one is the quantum mechanical version of the Hamilton-Jacobi equation of classical mechanics while the second is the quantum version of the Hamilton equations of motion. In quantum computation (at least in theory) we do not bother too much about these equations : we optimistically assume that if we need a specified U_t then somebody (a physicist, an engineer) will be able to construct a device (an electronic or optical device for example) which realizes the time evolution U. For us a specified time evolution is a *gate* that will ultimately be part of a quantum circuit.

It is very important to realize that *time evolution is linear*: this is quite surprising because in the classical regime one should get back the classical equations of motion which are generally non-linear[3].

Example 5. A semi-transparent mirror decomposes an incident ray into a reflected and a transmitted part (see chapter 1). Let $\mathcal{H} = \mathbf{C}^2$ the Hilbert space with basis $|T\rangle$, $|R\rangle$. The semi-transparent mirror acts in a unitary way

$$|T\rangle \to \boxed{\quad \mathrm{H} \quad} \to H|T\rangle = \frac{1}{\sqrt{2}}(|T\rangle + |R\rangle)$$

$$|R\rangle \to \boxed{\quad \mathrm{H} \quad} \to H|R\rangle = \frac{1}{\sqrt{2}}(|T\rangle - |R\rangle)$$

The unitary matrix H is called a Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

One checks that $HH^\dagger = H^\dagger H = 1$. If we put two semi-transparent mirrors in series (see exercises)

$$|\psi\rangle \to \boxed{\quad \mathrm{H} \quad} \to \boxed{\quad \mathrm{H} \quad} \to H^2|\psi\rangle = |\psi\rangle$$

the output is equal to the input because $H^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. In other words if the input state is $|T\rangle$ then the output is also $|T\rangle$. If we wish to take more seriously

[3] The study of this sort of reduction has led to a whole discipline called quantum chaos. Let us also point out that non-linear versions of the Schroedinger equation may arise when some degrees of freedom are integrated out, in other words for non-isolated systems.

into account the effect of the perfect mirrors in-between the semi-transparent mirrors, we insert between the two Hadamard matrices the gate $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$|\psi\rangle = \alpha|T\rangle + \beta|R\rangle \to \boxed{\text{ H }} \to \boxed{\text{ X }} \to \boxed{\text{ H }} \to HXH|\psi\rangle = \alpha|T\rangle - \beta|R\rangle$$

Principle 3: observable quantities. In quantum mechanics an observable quantity (energy, magnetic moment, position, momentum,...) is represented by a linear self-adjoint operator[4] on $\mathcal{H}$. For us this just means a hermitian matrix.

Examples 6.

- Position x, momentum $p = \frac{\hbar}{i}\frac{\partial}{\partial x}$, energy or Hamiltonian $\frac{p^2}{2m} + V(x)$. We will not need these.
- However we will need things like the polarization of a photon. Suppose we send a photon in a polarized beam-splitter (see chapter 1). If D_y clicks we record a -1 while if D_x clicks we record a $+1$. Our observations can be described by the observable

  $$\mathcal{P} = (+1)|x\rangle\langle x| + (-1)|y\rangle\langle y|$$

  This is the self-adjoint matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (in the $|x\rangle$, $|y\rangle$ basis).
- General observables in $\mathcal{H} = \mathbf{C}^2$ can always be represented by 2×2 hermitian matrices

  $$A = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \gamma \end{pmatrix}$$

  or in Dirac notation

  $$A = \alpha|0\rangle\langle 0| + \beta|0\rangle\langle 1| + \overline{\beta}|1\rangle\langle 0| + \gamma|1\rangle\langle 1|$$

  All such matrices can be written as linear combinations of

  $$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

  The observables (hermitian matrices !) X, Y, Z are called Pauli matrices. One of their uses is the description of the spin observable for spin $\frac{1}{2}$ particles: this is a "vector" with 3 components $\Sigma = (X, Y, Z)$. In the physics literature the notation is $\Sigma = (\sigma_x, \sigma_y, \sigma_z)$. Important properties of these matrices are

  $$X^2 = Y^2 = Z^2 = I,\ XY = -YX,\ XZ = -ZX,\ YZ = -ZY$$

  and

  $$[X, Y] = 2iZ,\ [Y, Z] = 2iX,\ [Z, X] = 2iY$$

[4] There is a "correspondence principle" which is a rule of thumb on how to construct the appropriate self-adjoint operator from the classical one; in fact this procedure may sometimes be a bit ambiguous due to non-commutativity of operators

This algebra is a special example of spin or Clifford algebras which play an important role in QM.

Principle 4: measurement postulate. This is the most disturbing postulate: it requires a rather big leap of intuition (or stroke of genius) which goes back to Max Born (one also speaks of the Born interpretation of the wave function). Let a system be prepared in a state $|\psi\rangle$. The system is to be measured with an apparatus. The apparatus is modeled by a set of orthonormal projectors $\{P_n\}$ satisfying $\sum_n P_n = I$. A single measurement *reduces*[5] the state ψ of the system to

$$|\phi_n\rangle = \frac{P_n|\psi\rangle}{||P_n|\psi\rangle||} = \frac{P_n|\psi\rangle}{\langle\psi|P_n|\psi\rangle^{1/2}}$$

For a single measurement *there is no way to predict* what will be the specific outcome n: it is random. If the experiment is repeated many times (assuming this is a reproducible experiment) one finds that the probability (in a frequentist interpretation of the term) of the outcome n is

$$\text{Prob}(\text{outcome } n) = |\langle\phi_n|\psi\rangle|^2 = \langle\psi|P_n|\psi\rangle$$

Remark 1. Since $\sum_j P_j = I$ and $|\psi\rangle$ are normalized we have $\sum_j \text{Prob}(\text{outcome } j) = 1$.

Remark 2. When the eigenprojectors are not degenerate these formulas are slightly simpler. If $P_j = |j\rangle\langle j|$ the probability of the outcome j is

$$\text{Prob}(\text{outcome } j) = \langle\psi|P_j|\psi\rangle = |\langle j|\psi\rangle|^2$$

and the state just after the measurement is $|j\rangle$.

Consequences for the measurement of observables. This is a very important point because ultimately one really measures physical quantities. The above measurement apparatus $\{P_n\}$ gives the value of any observable of the form $A = \sum_j a_j P_j$. The measurement makes $|\psi\rangle \to |\phi_n\rangle$ for some n. Since $A|\phi_n\rangle = a_n|\phi_n\rangle$ the value of A given by the measurement is precisely a_n when the outcome is n. In particular we can know simultaneously the value of many observables, by measuring them with the same appratus, as long as they have the same eigenspaces. Such observables commute and are sometimes said to be compatible.

The average value that the measurement, on the state $|\psi\rangle$, will yield can be calculated from the probability distribution above. One finds

$$\sum_j a_j \langle\psi|P_j|\psi\rangle = \langle\psi|A|\psi\rangle$$

[5] physicist are used to say that “the wave function collapses”

and the variance is

$$\sum_j a_j^2 \langle\psi|P_j|\psi\rangle - (\sum_j a_j \langle\psi|P_j|\psi\rangle)^2 = \langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2$$

In practice one uses the right hand side of these two formulas. That is basically all that a theorist can predict.

After a measurement the state vector is reduced $|\psi\rangle \to |\phi_n\rangle$, for some n, and thus the expectation value in the new state (i.e $|\phi_n\rangle$) becomes a_n and the variance 0. This means that if we repeat the same measurement on the same state we will get precisely the value a_n again and again.

We will return to this point when we will consider the Heisenberg uncertainty principle.

Example 7: measurement of photon polarization. Suppose we want to measure the observable $\mathcal{P} = |x\rangle\langle x| - |y\rangle\langle y|$ For this we use the apparatus constituted of an analyzer oriented along x and a detector. This apparatus is the physical realization of the measurement basis. If a photon is detected the state just after the measurement is $|x\rangle$ and if a photon is not detected (it has been absorbed by the analyzer) the state just after the measurement is $|y\rangle$. The probabilities of these outcomes are

$$\text{Prob(outcome } +1) = |\langle x|\psi\rangle|^2, \ \text{Prob(outcome } -1) = |\langle y|\psi\rangle|^2$$

If the initial preparation of the beam is $|\psi\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$ these probabilities are simply $\cos^2\theta$ and $\sin^2\theta$. Suppose that now we rotate the analyzer by an angle γ. This means that we wish to measure the observable $\mathcal{P} = |\gamma\rangle\langle\gamma| - |\gamma_\perp\rangle\langle\gamma_\perp|$. then we can compute again the probabilities of the outcomes

$$\text{Prob(outcome } +1) = |\langle\gamma|\psi\rangle|^2 = \cos^2(\theta-\gamma)$$

$$\text{Prob(outcome } -1) = |\langle\gamma_\perp|\psi\rangle|^2 = \sin^2(\theta-\gamma)$$

Finally let us note that in the first case the measured observable in matrix form is

$$\mathcal{P} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and in the second

$$\mathcal{P} = \begin{pmatrix} \cos 2\gamma & \sin 2\gamma \\ \sin 2\gamma & -\cos 2\gamma \end{pmatrix} = (\cos 2\gamma)Z + (\sin 2\gamma)X$$

Uncertainty principle Suppose that we have a system in a state ψ and we consider two observables A and B. We assume that these have spectral representations

$$A = \sum_j a_j P_j, \quad B = \sum_j b_j Q_j$$

As discussed previously in a general state $|\psi\rangle$ each of these is not fixed but has an average value $\langle\psi|A|\psi\rangle$, $\langle\psi|B|\psi\rangle$ and a standard deviation $\Delta A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$, $\Delta B = \sqrt{\langle\psi|B^2|\psi\rangle - \langle\psi|B|\psi\rangle^2}$. The Heisenberg uncertainty relation states that

$$\Delta A \cdot \Delta B \geq \frac{1}{2}\langle\psi|[A,B]|\psi\rangle$$

The interpretation of this inequality as first discussed by Heisenberg is that when $[A,B] \neq 0$ it is not possible to measure A and B simultaneously with infinite precision. If we manage to make $\Delta A = 0$ then we will have $\Delta B = \infty$. The prototypical and most striking example is $A = x$ (position) and $B = p = \frac{\hbar}{i}\frac{\partial}{\partial x}$ (momentum). In this case $\Delta x \Delta p \geq \frac{h}{4\pi}$ and we cannot measure simultaneously with infinite precision the position and the momentum of a particle: this is not a technological limitation but ultimately a “God given” limitation.

Note that if $[A,B] = 0$ then there exist a common basis of the Hilbert space in which A and B are both diagonal. Then by measuring in this basis, the measurement postulate tells us that both observables can be determined with infinite precision. There is no clash with the uncertainty relation because the right hand side of the inequality vanishes.

There is a related principle called the ”entropic uncertainty principle” which we now state. Suppose A and B have non degenerate eigenvalues

$$A = \sum_{n_a} a_{n_a}|n_a\rangle\langle n_a|$$

$$B = \sum_{m_b} b_{m_b}|m_b\rangle\langle m_b|$$

Set

$$H(A) = -\sum_{n_a} p(n_a)\ln p(n_a), \qquad H(B) = -\sum_{m_b} p(m_b)\ln p(m_b)$$

where

$$p(n_a) = |\langle n_a|\psi\rangle|^2, \qquad p(m_b) = |\langle m_b|\psi\rangle|^2$$

We have

$$H(A) + H(B) \geq -2\ln\big(\frac{1 + \max_{n_a,m_b}|\langle n_a|m_b\rangle|}{2}\big)$$

Principle 5: composite quantum systems. Suppose we have two systems $\mathcal{A}$ and $\mathcal{B}$ with Hilbert spaces $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$. The Hilbert space of the composite system $\mathcal{AB}$ is given by the tensor product space

$$\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$$

The states of $\mathcal{AB}$ are vectors $|\psi\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. The previous postulates apply to the composite system.

This is also a highly non trivial postulate as will be seen from its consequences throughout the course. In a famous paper Einstein, Podolsky, Rosen were the first to make a sharp analysis of its consequences. This has ultimately led to Bell inequalities and to important primitive protocols of quantum information such as teleportation and dense coding.

Example 8. Two photons with polarization degrees of freedom have Hilbert space $\mathbf{C}^2 \otimes \mathbf{C}^2$. Examples of states are $|x\rangle_{\mathcal{A}} \otimes |y\rangle_{\mathcal{B}}$ or $|x\rangle_{\mathcal{A}} \otimes |y\rangle_{\mathcal{B}} + |\theta\rangle_{\mathcal{A}} \otimes |\theta\rangle_{\mathcal{B}}$. N Qbits live in the space

$$\underbrace{\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes ... \otimes \mathbf{C}^2}_{N \text{ copies}}$$

If $|0\rangle, |1\rangle$ is a canonical basis for $\mathbf{C}^2$, a basis for the composite system is given by

$$|b_1\rangle \otimes |b_2\rangle ... \otimes |b_N\rangle = |b_1, ..., b_N\rangle$$

where $b_i = \{0, 1\}$. There are 2^N such states and they are in one to one correspondence with the 2^N classical bit strings of length N. A general N Qbit state is a linear superposition of the basis states:

$$|\psi\rangle = \sum_{b_1,...,b_N} c_{b_1,...,b_N} |b_1, ..., b_N\rangle$$

where the coefficients $c_{b_1...b_N}$ satisfy

$$\sum_{b_1,...,b_N} |c_{b_1,...,b_N}|^2$$

2.3 Tensor product versus entangled states

States of a composite system $\mathcal{AB}$ lie in $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. We say that a state is a *tensor product state* (or is *not entangled*) if it can be written as

$$|\psi\rangle = |\phi\rangle_{\mathcal{A}} \otimes |\chi\rangle_{\mathcal{B}}$$

An entangled state $|\psi\rangle \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ is one for which it is impossible to find $|\phi\rangle_{\mathcal{A}} \in \mathcal{H}_{\mathcal{A}}$ and $|\chi\rangle_{\mathcal{B}} \in \mathcal{H}_{\mathcal{B}}$ such that ψ is of the tensor product form.

Entangled states have very special correlations between their parts $\mathcal{A}$ and $\mathcal{B}$. These are genuine quantum correlations with no classical counterpart and as we will see later in the course they play a very important role (for example in teleportation). These definitions generalize to multipartite systems.

example 9. Two Qbit system with $\mathcal{A} \otimes \mathcal{B} = \mathbf{C}^2 \otimes \mathbf{C}^2$. Some product states are : $|0\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}} = |0, 0\rangle$, $|0\rangle_{\mathcal{A}} \otimes |1\rangle_{\mathcal{B}} = |0, 1\rangle$, $|1\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}} = |1, 0\rangle$, $|1\rangle_{\mathcal{A}} \otimes |1\rangle_{\mathcal{B}} = |1, 1\rangle$. Two less trivial ones are

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} + |1\rangle_{\mathcal{B}}) \otimes |0\rangle_{\mathcal{B}} = \frac{1}{2}(|0, 0\rangle + |1, 0\rangle)$$

and

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} + |1\rangle_{\mathcal{B}}) \otimes \frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{B}} - |1\rangle_{\mathcal{B}}) = \frac{1}{2}(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle)$$

In the same space there are also entangled states that simply *cannot* be written as a tensor product form. For example,

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}} + |1\rangle_{\mathcal{A}} \otimes |1\rangle_{\mathcal{B}}) = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}} - |1\rangle_{\mathcal{A}} \otimes |1\rangle_{\mathcal{B}}) = \frac{1}{\sqrt{2}}(|0,0\rangle - |1,1\rangle)$$

$$\frac{1}{\sqrt{2}}(|1\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}} + |0\rangle_{\mathcal{A}} \otimes |1\rangle_{\mathcal{B}}) = \frac{1}{\sqrt{2}}(|1,0\rangle + |0,1\rangle)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}} - |1\rangle_{\mathcal{A}} \otimes |0\rangle_{\mathcal{B}}) = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$$

As we will see these four particular states play a special role and are called Bell states. The reader can check that they form a basis of the 2 Qbit space.

Production of entangled states. Suppose we have a composite system in an initial tensor product state $|\phi\rangle_{\mathcal{A}} \otimes |\chi\rangle_{\mathcal{B}}$. These could for example be two electrons in the spin state $|\uparrow\rangle \otimes |\downarrow\rangle$. If we let them evolve separately and without interaction, the unitary operator for the time evolution is of the form $U_{\mathcal{A}} \otimes U_{\mathcal{B}}$ and

$$U_{\mathcal{A}} \otimes U_{\mathcal{B}}(|\uparrow\rangle \otimes |\downarrow\rangle) = U_{\mathcal{A}}|\uparrow\rangle \otimes U_{\mathcal{B}}|\downarrow\rangle$$

so that the system remains in a tensor product state.

Thus to produce entangled states systems $\mathcal{A}$ and $\mathcal{B}$ must interact at some point in time in order to have an evolution $U_{\mathcal{AB}} \neq U_{\mathcal{A}} \otimes U_{\mathcal{B}}$. With an appropriate interaction we might be able to achieve

$$U_{\mathcal{AB}}(|\uparrow\rangle \otimes |\downarrow\rangle)$$

All known physical interactions are local: this means that in order to interact (in a non-negligible way) two systems must be ”close in space-time”. In particular if we are presented with an entangled state we know that the two parties have interacted in the past, i.e they have been ”sufficiently close in the past”.

2.4 No cloning theorem

Classical bits can be copied. For example any latex file can be duplicated or any text can be copied with a (universal) Xerox machine.

Suppose we have a set of quantum states $|\psi\rangle \in \mathcal{H}$ and we want to build a (universal) ”quantum Xerox machine” to copy $|\psi\rangle$. This machine should be able to copy any state of $\mathcal{H}$. A quantum Xerox machine should be described by some unitary operator U (this is true for any physical process except measurement). The Hilbert space is composite $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ where $\mathcal{A}$ is the quantum file to be copied and $\mathcal{B}$ the duplicated file. We start from the state

$$|\psi\rangle \otimes |\text{blank}\rangle$$

and we feed it in the Xerox machine

$$|\psi\rangle \otimes |\text{blank}\rangle \rightarrow \boxed{\quad \text{U} \quad} \rightarrow |\psi\rangle \otimes |\psi\rangle$$

In mathematical terms the question is: can one find a unitary operator such that for a reasonably large set of ψ

$$U(|\psi\rangle \otimes |\text{blank}\rangle) = |\psi\rangle \otimes |\psi\rangle$$

The answer is NO and this is sometimes called the "no cloning theorem". However it is possible to copy a set of orthogonal states with an appropriate U depending on the set.

Proof of no-cloning theorem. Suppose there exists U such that $U^\dagger U = UU^\dagger = 1$ with

$$U(|\phi_1\rangle \otimes |\text{blank}\rangle) = |\phi_1\rangle \otimes |\phi_1\rangle$$

$$U(|\phi_2\rangle \otimes |\text{blank}\rangle) = |\phi_2\rangle \otimes |\phi_2\rangle$$

conjugating the second equation

$$(\langle\phi_2| \otimes \langle\text{blank}|)U^\dagger = \langle\phi_2| \otimes \langle\phi_2|$$

Taking the inner product with the first equation

$$\langle\phi_2| \otimes \langle\text{blank}|U^\dagger U|\phi_1\rangle \otimes |\text{blank}\rangle = (\phi_2| \otimes \langle\phi_2|)(|\phi_1\rangle \otimes |\phi_1\rangle)$$

which implies

$$\langle\phi_2|\phi_1\rangle\langle\text{blank}|\text{blank}\rangle = \langle\phi_2|\phi_1\rangle^2$$

so

$$\langle\phi_2|\phi_1\rangle = 0 \text{ or } \langle\phi_2|\phi_1\rangle = 1$$

We conclude that we cannot copy states $|\phi_1\rangle$ and $|\phi_2\rangle$ that are not identical or orthogonal, with the same U. In fact it is possible to copy a given orthogonal basis . To see this the reader has to construct a unitary operation that does the job.

Non orthogonal states cannot be perfectly distinguished. There are many variants and refinements of the no-cloning theorem. let us just show one such variant. Suppose we have two states $|\psi\rangle$ and $|\phi\rangle$ and we want to build a (unitary) machine to distinguish them. We seek a U such that

$$U|\psi\rangle \otimes |a\rangle = |\psi\rangle \otimes |v\rangle$$

$$U|\phi\rangle \otimes |a\rangle = |\phi\rangle \otimes |v'\rangle$$

where the outputs $|v\rangle$ and $|v'\rangle$ give some information about $|\psi\rangle$ and $|\phi\rangle$. Taking the inner product of these two equations yields

$$\langle\phi| \otimes \langle a|U^{\dagger}U|\psi\rangle \otimes |a\rangle = (\langle\phi| \otimes \langle v'|)(|\psi\rangle\rangle \otimes |v\rangle)$$

This implies

$$\langle\phi|\psi\rangle\langle a|a\rangle = \langle\phi|\psi\rangle\langle v'|v\rangle$$

If $|\phi\rangle$ is not orthogonal to $|\psi\rangle$ we have $\langle\phi|\psi\rangle \neq 0$ thus

$$\langle v'|v\rangle = \langle a|a\rangle = 1$$

Thus $|v\rangle = |v'\rangle$ so there is no information in $|v\rangle$ and $|v'\rangle$ distinguishing $|\psi\rangle$ and $|\phi\rangle$.

3 Quantum key distribution

One of the first applications of quantum mechanics to the field of information theory has been the 1984 proposal of Bennett and Brassard for a secure protocol to distribute a secret key that is common to two distant parties. Since then, there have been a few other similar protocols and a new field has emerged, called "quantum cryptography". In this chapter we limit ourself to the original protocol - now called BB84 - and to a simpler one found by Bennet in 1992. In a later chapter we will also give another protocol proposed by Ekert in 1991, and based on entangled Einstein-Podolsky-Rosen pairs of particles.

The general idea of BB84 is as follows. Alice sends a string of classical bits - the secret key - to Bob by using intermediate quantum mechanical Qbits (in practice these are photons transmitted in optic fibers). Any attempt by Eve to capture some information about the key amounts to *observe* the Qbits, but according to the postulates of QM *this observation will perturb the quantum system.* Alice and Bob are then able to detect this perturbation, thus the presence of Eve, and abort communication.

The subject is in fact more complicated because in reality the channel (the optic fiber) is noisy and it is non-trivial to distinguish Eve from noise. Besides the operations performed by Alice and bob are not perfect. The proof of security (see [?]) for BB84 is therefore dependent on precise assumptions on the physical set-up. It involves a combination of non-trivial methods from classical and quantum information theory and is beyond the scope of this course. Here we will analyze only two basic attacks from Eve, assuming the channel is not noisy and the operations of Alice and Bob are perfect.

Quantum cryptography is not only a theoretical idea. It is also a truly experimental subject since the protocols have been implemented and shown to work in the laboratory (first at IBM in 1989 over a distance of 32 cm) and later outside the lab on distances of few tens to hundreds of kilometers (Geneva, Los Alamos ...). See [?] for a general review. Nowadays there exist companies proposing commercial systems[1]. Recent implementations allow the exchange of secret keys over a distance of $100km$ (resp. $250km$) at a rate of 6000 (resp. 15) bits per second [?]. require extensive knowledge of optics and will not be discussed here. Recently the commercial systems have been challenged by a hacking procedure exploiting the physical limitations of photo-detectors on Bob's side [?].

[1] Idquantique, MagiQ

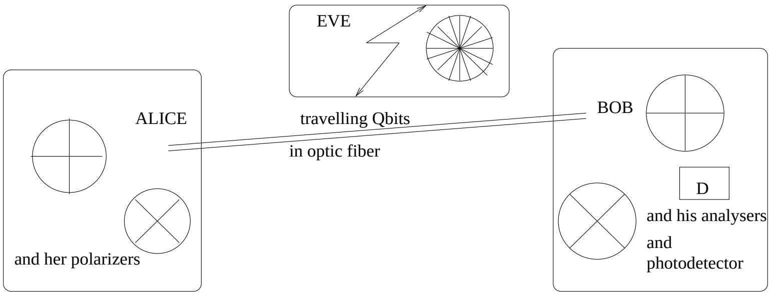

Figure 3.1 Alice and Bob exchange a private key over an optic fiber

Figure 3.2 orientations of polarizer for preparation of photons in Z basis

3.1 Key generation according to BB84

There are four essential phases: the encoding procedure of Alice, the decoding procedure of Bob, a public discussion between the two parties, and finally the common secret key generation. Figure 3.1 illustrates the general set-up described below.

Encoding procedure of Alice. She generates a classical random binary string $x_1, ..., x_N$, $x_i \in \{0,1\}$ that she keeps secret. The common key will be a subset of these bits. She also generates a second classical random binary string $e_1, ..., e_N$, $e_i \in \{0,1\}$ that she keeps secret *for the moment.* Alice then *encodes* the classical bits x_i into Qbits as follows:

- For $e_i = 0$ she generates a Qbit in the state $|x_i\rangle$. Concretely this can be done by sending a beam through a polarizer in the Z basis (figure 3.2)

$$\{|0\rangle, |1\rangle\}$$

  For $x_i = 0$ (resp. $x_i = 1$) the polarizer is oriented horizontally (resp. vertically) and so photons are prepared in polarization state $|0\rangle$ (resp. $|1\rangle$). A single photon is then selected from the outgoing beam (this of course is an idealization)
- For $e_i = 1$ she generates a Qbit in the state*[2] $H|x_i\rangle$. Concretely this can be

[2] We remind the reader that H is the Hadamard matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

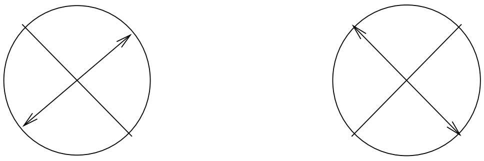

Figure 3.3 orientations of polarizer for preparation of photons in X basis

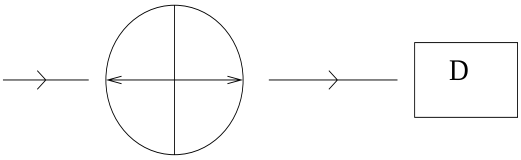

Figure 3.4 analyzer-detector set-up for the measurement of polarization in Z basis

done by sending photons through a polarizer in the X basis (figure 3.3

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

For $x_i = 0$ (resp,. $x_i = 1$) the polarizer is rotated to the right (resp. left) and photons are prepared in polarization state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (resp. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$).

Summarizing, Alice sends a string of Qbits $|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$, $i = 1, ..., N$ through a channel (in practice the channel is an optical fiber).

Decoding procedure of Bob. Bob generates a random classical binary string $d_1, ..., d_N$, $d_i \in \{0, 1\}$ that he keeps secret *for the moment*. He decodes the received Qbits of Alice as follows:

- If $d_i = 0$ he performs a measurement of the received Qbits $|A_{e_i,x_i}\rangle$ in the Z basis

  $$\{|0\rangle, |1\rangle\}.$$

  The photon state after the measurement

  $$|y_i\rangle \in \{|0\rangle, |1\rangle\}.$$

  is recorded in the bit y_i. To do this concretely he uses the analyzer-detector apparatus described in the first chapter: the analyzer is placed horizontally (figure 3.4); if the detector clicks this means the photons state has *collapsed* in the $|0\rangle$ state and if the detector does not click, it means that the photon state has collapsed to $|1\rangle$. We stress that, according to the measurement postulate, these outcomes are *truly random*. Only Bob knows about them.

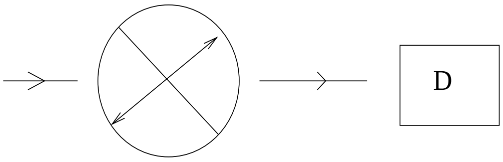

Figure 3.5 analyzer-detector set-up for the measurement of polarization in X basis

- If $d_i = 1$ he performs a measurement of the received Qbits $|A_{e_i,x_i}\rangle$ in the X basis

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle\}.$$

The photon sate after the measurement is in

$$H|y_i\rangle \in \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

When the output is $H|y_i\rangle$, and he records the bit y_i.

To do this concretely he uses the analyzer-detector apparatus described in the first chapter: the analyzer is rotated to the right (figure 3.5) at 45 degrees; if the detector clicks this means the photons state has *collapsed* in the $H|0\rangle$ state while if the detector does not click it means that the photon state has collapsed to $H|1\rangle$. We stress again that, according to the measurement postulate, these outcomes are *truly random* and that only Bob knows about them.

In summary Bob has decoded the Qbits sent by Alice to a classical binary string $y_1, ..., y_N$. This string is the outcome of measurements of Bob and cannot be predicted (God does play with dice ... the statistics of the outcomes can however be calculated according to the measurement postulate).

Public discussion. Alice has at her disposal two binary strings: $e_1, ..., e_N$ used to choose the encoding basis, and $x_1, ..., x_N$ that was mapped to Qbits. Bob also has two binary strings: $d_1, ..., d_N$ used to choose a measurement basis and $y_1, ..., y_N$ that are his measurement outcomes.

Alice and Bob compare $e_1, ..., e_N$ and $d_1, ..., d_N$ over a public channel, but keep their two other strings $x_1, ..., x_N$ and $y_1, ..., y_N$ secret. *It important that the public discussion starts only after Bob has finished his measurements.* They can deduce the following information (and anybody else hearing the public discussion also can):

- If $d_i = e_i$, i.e. if they used the same basis, then it must be the case that $y_i = x_i$ (the reader should convince himself of that by going through some examples with polarizer, analyzer pairs - basically if Bob and Alice used the same basis it is as if they lived in a classical world).
- If $d_i \neq e_i$, i.e. if they did not use the same basis, then genuine quantum effects

came into play when Bob did the measurement. According to the measurement postulate: $y_i \neq x_i$ with probability $\frac{1}{2}$ and $y_i = x_i$ with probability $\frac{1}{2}$. Let us formally prove this. Bob receives the Qbit

$$|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$$

and measures in the basis

$$\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}.$$

The outcome will be one of two basis states

$$H^{d_i}|0\rangle, \qquad \text{with prob } |\langle 0|H^{d_i}H^{e_i}|x_i\rangle|^2$$

or

$$H^{d_i}|1\rangle, \qquad \text{with prob } |\langle 1|H^{d_i}H^{e_i}|x_i\rangle|^2.$$

The reader can check that for $e_i \neq d_i$ both probabilities are equal to $\frac{1}{2}$ (and that for $e_i = d_i$ they are 0 and 1).

Key generation. Bob and Alice erase all bits x_i and y_i corresponding to i such that $e_i \neq d_i$. They keep the remaining sub-strings of $x_1, ..., x_n$ and $y_1, ..., y_n$ such that $e_i = d_i$. They are assured that these two sub-strings are identical, so this can potentially constitute the common secret key. The length of this sub-string is close to $\frac{N}{2}$ since prob$(e_i \neq d_i) = \frac{1}{2}$. Finally Alice and Bob perform a security test: according to quantum mechanics for this perfect setting (without noise or Eve) one must have

$$\text{prob}(x_i = y_i | e_i = d_i) = 1$$

Alice and Bob test this by exchanging a small fraction of the common sub-string over the public channel. If the test succeeds they keep the rest of the common sub-string secret: they have succeeded in generating a common secret key.

3.2 Attacks from Eve

We assume that Alice has a perfect single-photon source, state preparation is perfect, there is no channel noise, Bobs analyzer-detector apparatus makes no detection errors. In summary when Eve is absent communication is error-free, and any error discovered in the security test would come from Eve. Furthermore we suppose that Eve may attack by performing operations on one Qbit at a time on captured photons along the optic fiber and that she has no access to the Alice and Bob's labs. We also suppose that Eve has perfect knowledge of the set-up in Alice and Bob's labs: she knows that they use X and Z basis (but not the successive random basis choices), she knows what is their common vertical and horizontal directions, and the timing of the photons.

We consider two possible attacks : “the measurement” and “unitary” attacks.

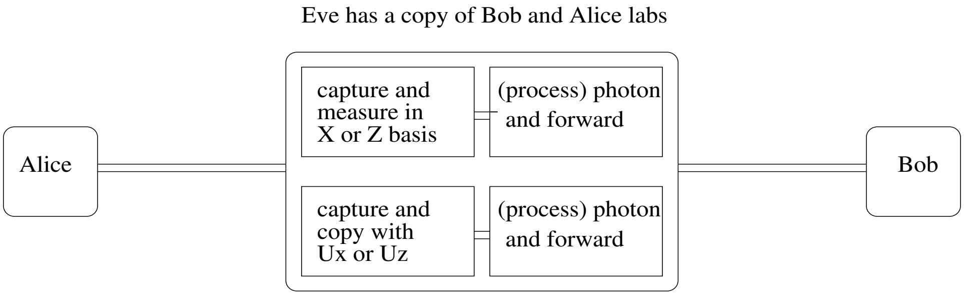
Eve has a copy of Bob and Alice labs
capture and measure in X or Z basis
(process) photon and forward
Alice
Bob
capture and copy with Ux or Uz
(process) photon and forward

Figure 3.6 Set up of Eve's lab along the optic fiber

The two attacks consist of two steps. First Eve captures a photon, and second she forwards the photon to Bob (see figure 3.6). For each attack we will see that the basic postulates of QM imply that Bob and Alice discover the presence of Eve. when this is the case they abort the protocol.

Measurement attack. Suppose Eve captures a single photon in the optic fiber. The captured photon is in one of the the states

$$|A_{e_i,x_i}\rangle \in \big\{|0\rangle, |1\rangle, H|0\rangle, H|1\rangle\big\}$$

and she tries to measure it. If Eve uses the Z basis her outcome is in $\{|0\rangle, |1\rangle\}$ and according to it she records a bit $y_i^E \in \{0,1\}$. If she uses the X basis her outcome is in $\{H|0\rangle, H|1\rangle\}$ and she records a corresponding bit $y_i^E \in \{0,1\}$. Once she has finished the measurement she sends the photon to Bob in the state left over by the measurement[3]. Two possibilities may occur:

- Eve has used the same basis than Alice: then her outcome is $y_i^E = x_i$ and the photon state received by Bob is the "correct one".
- Eve uses a different basis than Alice: then her outcome $y_i^E = x_i$ only half of the time, so she sends the "correct" photon state to Bob only half of the time.

Let us see what Alice and Bob find when they perform the security test. Denote by EA the event "Eve uses the same basis than Alice".

$$\begin{aligned}\text{prob}(x_i = y_i | e_i = d_i) &= \text{prob}(x_i = y_i | e_i = d_i, EA)\text{prob}(EA) \\ &\quad + \text{prob}(x_i = y_i | e_i = d_i, \text{not}\, EA)\text{prob}(\text{not}\, EA) \\ &= 1 \cdot \text{prob}(EA) + \frac{1}{2} \cdot (1 - \text{prob}(EA)) \\ &= \frac{1}{2}(1 + \text{prob}(EA))\end{aligned}$$

[3] She could also further process this state by a unitary transformation but this will not improve her performance

where we used

$$\text{prob}(x_i = y_i | e_i = d_i, EA) = 1, \qquad \text{prob}(x_i = y_i | e_i = d_i, \text{not EA}) = \frac{1}{2} \quad (3.1)$$

Assuming that Eve has no information about the basis choices of Alice we take $\text{prob}(EA) = \frac{1}{2}$. Then

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}$$

so that Alice and Bob notice that when they used the same basis about a fourth of their bits do not agree. They conclude that an eavesdropper is at work and abort the communication.

Unitary attack. The problem of Eve is that when she makes a measurement she has no information about the basis that Alice chose. One possible solution would be to copy the traveling Qbits $|A_{e_i,x_i}\rangle$, then let the original state go to Bob, and keep the copy. When Alice and Bob enter in the public discussion phase she learns about the basis of Bob in which to measure the Qbit and thus for i such that $e_i = d_i$ she gets the same outcome as Bob $y_i^E = y_i = x_i$.

However the *no-cloning theorem* (which is a consequence of the unitary evolution postulate) guarantees that there does not exist a unitary ”machine“ such that

$$U(|A_{e_i,x_i}\rangle \otimes |\text{blank}\rangle) = |A_{e_i,x_i}\rangle \otimes |A_{e_i,x_i}\rangle$$

The point here is that $|A_{e_i,x_i}\rangle$ is one of

$$\{|0\rangle,\ |1\rangle,\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

which is a set of non-orthogonal states.

Eve could try to use two copy machines: one for copying the two states of the Z basis and another for copying the two states of the X basis. But this time she has no way of knowing which machine to use. She will use the wrong machine half of the time and again Alice and Bob will find that

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}$$

Discussion of security issues. In the above error-free set-up it is relatively easy to generalize the proof of security in order to take into account any local operation of Eve on single photons. In a more realistic context one has to take into account the fact that the system is noisy. For example the optic fiber is not perfect and the photo-detectors may give false counts. Therefore the string sequences of Alice and Bob do not match perfectly even when $e_i = d_i$. For this reason one adds to the protocol two classical post-processing steps: information reconciliation and privacy amplification. Both steps are carried on the public classical channel. The first step is an error correcting phase while the second allows to reduce the information that Eve might have gained about the key during the correction phase. The detailed analysis is non-trivial and the interested reader may consult the literature [**?**].

There are various problems that may arise due to physical limitations that do not quite enter into the framework of the security proofs. Recently a successful attack was implemented [**?**] by exploiting the fact that after a photo-detector click, the detectors enter in a mode were they operate classically. By shining light on them Eve is able to maintain them in a classical mode and in effect the Eve-Bob part of the transmission line is in effect classical. In this Eve can achieve complete control of the key.

3.3 The Bennett 1992 scheme

The analysis of BB84 has shown that the security ultimately relies on the fact that Alice encodes Qbits in non-orthogonal states. The B92 scheme retains this very fact and is even simpler than BB84. Below we just sketch the main idea. There are again four main phases:

Alice encodes. Alice prepares a random binary string $e_1, ..., e_N$. She sends to Bob $|A_{e_i}\rangle = |0\rangle$ if $e_i = 0$ and $|A_{e_i}\rangle = H|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ if $e_i = 1$. The encoding is thus $H^{e_i}|0\rangle$.

Bob decodes. Bob generates a random binary string $d_1, ..., d_N$ and measures the received Qbit according to the value of d_i in the Z or X basis and obtains an outcome in $\{|0\rangle, |1\rangle\}$ or in $\{H|0\rangle, H|1\rangle\}$. He decodes the bit as $y_i = 0$ if the outcome is $|0\rangle$ or $H|0\rangle$ and $y_i = 1$ if the outcome is $|1\rangle$ or $H|1\rangle$.

Public discussion. Bob announces over the public channel the bits y_i. Note that when $e_i = d_i$ we have $y_i = 0$ with probability 1. On the other hand when $e_i \neq d_i$ we have $y_i = 0$ with probability $\frac{1}{2}$ and $y_i = 1$ with probability $\frac{1}{2}$. Therefore from the public discussion Alice and Bob deduce that, given $y_i = 1$, surely $d_i = 1 - e_i$.

Key generation. Alice and Bob keep the secret bits $(e_i, d_i = 1 - e_i)$ for i such that $y_i = 1$ and discard the rest. The length of this sub-string is about $\frac{N}{2}$. they perform a security test on a fraction of the sub-string on the public channel by checking that

$$\text{prob}(d_i = 1 - e_i | y_i = 1) = 1$$

Again it is not hard to check that this security condition is violated under a measurement or a unitary attack of Eve. If that is the case Alice and Bob abort communication.

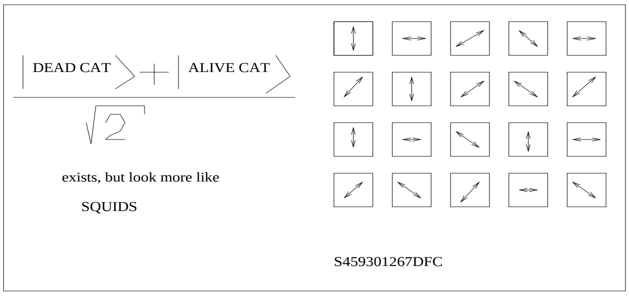

Figure 3.7 unforgeable bank note: it buys one Schroedinger cat

3.4 Conjugate coding

In the encoding method of Alice above the two basis that are used correspond to the basis diagonalizing the two Pauli matrices

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.2}$$

These two observables do not commute and are called conjugate observables by analogy with position and momentum; therefore the two basis are sometimes called *conjugate* and the corresponding scheme called *conjugate coding.*

In fact this scheme was first introduced in 1969 by Wiesner then a graduate student. Wiesner, basing himself on the principles of QM, indicated how to ”fabricate unforgeable bank notes“. Unfortunately nobody took him seriously, except for Bennett then also a graduate student, and his paper didn't get published till*[4] 1983. Bennett was one of the few persons who kept thinking about such problems and, with Gilles Brassard a computer scientist, had the idea to reconsider conjugate coding in the context of cryptography.

Let us briefly explain the original idea of Wiesner. One generates a random binary string $e_1, ..., e_{20}$, and prepares 20 photons in $|0\rangle$, $|1\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, polarization states using Z or X polarizers. Then one traps the 20 photons in 20 small cavities inside the bank note. The bank note also contains a readable serial number which corresponds to the binary string $e_1, ..., e_{20}$. Only the bank knows what is the mapping between the serial number and the binary string (see figure 3.7).

Suppose somebody attempts to copy the bank note. Because of the no-cloning theorem there is no single machine U which copies simultaneously vertical and diagonal photon polarizations. If one uses two different machines one will make mistakes (with prob $1 - 2^{-20}$) because one doesn't know when to use a U_Z or a U_X. Moreover the bank can check if a bank note has been forged or not. Indeed from the serial number it deduces the binary string $e_1, ..., e_{20}$ and therefore

[4] around 1982 quantum computation came into fashion because of an equally pioneering work of Feynman

knows the basis sequence used to prepare the photons. A measurement in the correct basis (for each little cavity) is done to observe if the photons have the correct polarization. Note that if the bank note has *not* been forged it will *not* be destroyed by such a procedure. To summarize, one may say that the bank knows what exact sequence of analyzers to use so that the system behaves classically for the bank. For any other person that does not possess this information the system behaves quantum mechanically.

Part II

Quantum Information Theory

Part III

Quantum Computation

Notes